Optima Technology Information Security Whitepaper

optima
technology

Introduction

Optima delivers world-class and efficient software for the management and analysis of utility data. For our customers - many of whom are amongst the UK's largest energy users and best-known utilities consultancies – it's critical to understand the detail of how we deliver optimum security.

To protect the privacy of its customers and the safety of their information, Optima relies upon state-of-the-art and secure data centres, enforces strict internal product controls, and regularly audits its policies and procedures using third-party auditors.

The key principles of Optima's security strategy of Infor Birst's security are:

- Security is designed from the ground up in the application, network, hardware, and operational procedures.
- Optima is ISO 27001, ISO 22301, ISO 9001 and Cyber Essentials Plus certified.
- We use modern, Tier-4 data centres that are SOC 2 Type 2 audited and are ISO 27001 certified or follow ISO 27001 policies.
- Adherence to security best practices for code development, testing, and operations is followed.
- Regular external review of the policies and procedures for security and operations are conducted.
- Regular penetration and vulnerability testing by third parties is completed.

The following sections of this document cover the key areas of Optima's security strategy in detail and describe how we utilise a 'defence in depth' methodology, which refers to applying layers of security to avoid a single point of failure. These layers are defined as:

- **Organisational** - Controls to ensure that we operate with processes, policies and procedures designed to embed protection against risk and achieve resilience and compliance throughout the organisation.
- **People** - Providing our people with the necessary tools to enable them to design, develop and deliver the organisation's products and services whilst maintaining security.
- **Physical** - Addressing the risks to facilities and equipment where our data is processed to protect from physical damage, unauthorised access or failure.
- **Technological** - Building security controls into our environments and customer-facing applications, reducing their exposure to vulnerabilities and meeting the expectations of our customers.

Organisational Security

Internal Systems

All communications with externally facing systems (e.g. email, SFTP, web) are encrypted at the transport level. Optima's cloud-based user systems (such as Google Workspace) are also encrypted at the transport level. VPN connections to our company network are secured via a combination of a pre-shared key and username and password. Multi-factor authentication is enabled on applications where this is supported by the vendor.

Encryption

At a company level, all of our information hardware assets (laptops and mobile devices) are encrypted at the system level as part of the setup process using Optima's chosen encryption application.

Firewalls

High performance firewalls are installed at our office and cloud hosting. This protects our infrastructure and the information that we manage for ourselves and our customers. We have scheduled reviews of firewall rules and configuration. The firewall administrative interface is protected from direct access via the internet.

Endpoints

Workstations are configured using Optima's baseline standard for security using the principle of least privilege. Each workstation is tracked and monitored by endpoint management solutions and are required to have strong passwords. It is company policy that workstations must be locked when idle.

Optima maintains a dynamic asset inventory which documents all information assets belonging to the company.

All of our workstations have a properly configured host-based firewall within the network. Each workstation has a properly configured host-based firewall when connected to untrusted networks such as public wi-fi hotspots.

Antivirus

Optima's endpoints have anti-virus software installed; administered by our IT team. This enables the reporting of potential malware, unauthorised software and ensures restrictions from running mobile storage devices. All downloaded files and software will be scanned by endpoint security protection software. Our email system is set up to scan all incoming email for malicious software and anything that appears to be suspicious will be quarantined if necessary.

Full antivirus and malware scans are run weekly on all devices (the scope of these scans will be defined per device group). The schedule and scope of these scans are detailed and maintained by our IT department.

Vulnerability Management

We have measures to detect and prevent the introduction of malicious software into our information processing systems, using endpoint security protection and system monitoring tools to create alerts which are promptly investigated and resolved. Full antivirus and malware scans are run weekly on all devices (the scope of these scans will be defined per device group). All downloaded files and software are scanned by endpoint security protection software.

The email system is set up to scan all incoming email for malicious software and is quarantined if necessary. Optima has a procedure to follow in the event of a virus outbreak to contain and remove it.

Vulnerabilities are categorised using the Common Vulnerability Scoring System (CVSS) and are a way of capturing the principal characteristics of vulnerabilities and to produce a numerical score reflecting its severity. Vulnerabilities are remediated with critical and high-level vulnerabilities being treated as a priority.

Mobile Devices

We do not allow the use of personal devices for any work activity. For roles which require them, mobile devices are enrolled in the company's mobile device management system which allows remote wiping of the device.

Access Rights

Access rights to the Optima network are controlled by role using group policy in order to prevent unauthorised access to information held in application systems. Systems and applications which are used by Optima are documented to show which systems are required by each user and their required level of access. User accounts are administered by our IT team and are set up using a least-privileged account for day-to-day operations.

User Authentication

We enforce a strict password policy which requires all of our personnel to use a centrally managed system that stores and encrypts passwords. This system allows the random generation of passwords using all character types to different password lengths. Each user has their own password management accounts; and multi-factor authentication is enabled.

We also have a documented password policy which clearly sets out the enforced procedures for password and secret authentication information management.

To further reduce risk, we utilise multi-factor authentication on systems where it is available such as for third-party web applications which are used for general day to day business operations. All company laptops are secured using full volume encryption which requires user authentication on start-up.

System Monitoring

Optima has a number of methods for reporting and responding to technical vulnerabilities. These include:

- Subscription to a Cloud-based Vulnerability Management Platform;
- Optima Antivirus Solution is pushed out and weekly scheduled scans take place;
- Windows updates are pushed out to information assets;
- Monitoring of assets to ensure latest version updates and patches are installed;
- Notifications from Special Interest Groups;
- Annual Penetration Testing;
- Cyber Essentials Plus accreditation;
- Monitoring of media including television, radio, internet and social media.

Scanning and Alerting

We have measures to detect and prevent the introduction of malicious software into our information processing systems, using endpoint security protection and system monitoring tools to create alerts which are promptly investigated and resolved.

Backups

Optima's head office infrastructure is backed up at the virtual machine level. Our Backup Policy retains daily backups which are stored in a Microsoft Azure data centre. Production Servers requiring backup are added to an Azure Recovery Services policy.

Supplier Management

We regularly perform due diligence checks on our supply chain to ensure our security posture is maintained. If security controls are inadequate for the proportionate level of data the supplier may process, we seek enhanced controls or further verification to countermeasure the perceived risk to Optima.

When selecting an application or information system to be used for business efficiency or to enhance our development and site reliability, we have an established criteria for assessing the security posture of a product prior to use. This is to ensure that security processes are embedded into the software and to prevent any security vulnerabilities from impacting Optima's infrastructure.

Cyber Essentials Plus

Cyber Essentials Plus ensures that Optima is guarded against common cyber threats and is independently verified through technical tests which assess the posture of our controls. Certification is assessed and awarded on an annual basis.

The Cyber Essentials scheme is Government-backed and is formally recognised as a certification for best practice cyber security. Cyber Essentials Plus provides assurance to our company stakeholders of Optima's commitment to cyber security.

A copy of our Cyber Essentials Plus certificate can be obtained on request.

ISO 27001

Optima's Information Security Management System is certified to IEC/ISO 27001, the international standard for information security. The objectives are to ensure availability of our software products, to protect the confidentiality, integrity and availability of data and to continually improve Optima's ISMS.

Our certificate is awarded by the British Standards Institute (BSI) and is independently audited twice per year, with a full recertification taking place every three years.

The certification applies to our UK operation, with the scope: "The design, development and maintenance of energy analysis software products to industries with utility management solutions, in the UK."

A copy of our ISO 27001 certificate can be obtained on request.

Privacy Policy

Our privacy policy sets out very clearly how we handle the personal data we collect and hold about individuals. This policy also explains your privacy rights and how the law protects you, including how we comply with the General Data Protection Legislation.

Our Privacy Policy is available to read on our website.

People Security

Internal Security Team

We employ a full-time Compliance Manager who is responsible for the management of the information security system and overarching strategy to protect the company's information assets. Our information security department is overseen by Optima's Senior Leadership Team and technical implementation is managed by our Site Reliability Engineering Team. External validation is given by auditors and consultants who visit our office to carry out detailed security audits and tests to certify our information security processes.

Our Compliance Manager is a Lead Implementer and Internal Auditor for ISO 27001, certified by the British Standards Institution.

Security Awareness Training

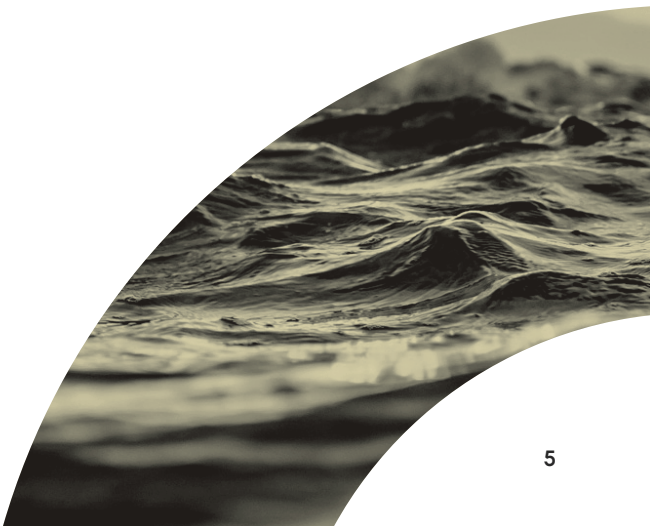
We organise quarterly awareness briefings for all of our employees to ensure they are aware of (and understand the wide-reaching implications of) the information security landscape. These sessions have multiple benefits. They provide an opportunity to involve our employees in the continual development of our information security plans; they are a useful forum to gather feedback on the performance of the management system; and they are key to improving the culture and communication within our organisation.

Secure Development Training

To up-skill our technical and specialist teams, training is provided to ensure they continue to grow their knowledge and develop their expertise in a dynamic industry. For example, our development team has attended practical security courses where they were taught how to implement offensive skills into the development stage with a view to combating security vulnerabilities throughout the process.

Professional Development

We see the continual development of our technical staff as a key element of our security strategy. We know that the software development life cycle is dynamic, and therefore it's essential for us to ensure that our developers are highly-skilled in security. Our staff regularly attend conferences and training courses – many of which are led by the world's leading thinkers and experts in the field of data security. This knowledge allows our technical teams to incorporate secure coding techniques into the build stage; encourages security by design; and advances the security of our software and allows us to deliver a robust product to our customers more quickly.



Physical Security

Production Environment

Our software is hosted using the Microsoft Cloud Azure platform. Our data centres are situated in the EU, utilising geo-redundancy in case of a site failure.

Microsoft Azure meets a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards, such as Australia IRAP, UK G-Cloud and Singapore MTCS.

Microsoft Azure provides businesses with the data security and privacy, control, and transparency they require. Security and privacy are embedded in the Microsoft Azure platform using the Security Development Lifecycle (SDL).

Microsoft Azure uses multiple safeguards to protect customer and enterprise data. These security practices and technologies include:

- **Encription** – Microsoft Azure uses industry-standard protocols to encrypt data as it travels between devices and Microsoft data centres, and crosses within data centres
- **Secure Networks** – Microsoft Azure infrastructure relies on security practices and technologies to connect virtual machines to each other and to on-premises data centres, while blocking unauthorised traffic.
- **Threat Management** – Microsoft Antimalware protects Azure services and virtual machines. Microsoft also uses intrusion detection, denial-of-service (DDoS) attack prevention, penetration testing, data analytics, and machine learning to constantly strengthen its defence and reduce risks.
- **Compliance** – Microsoft Azure complies with both international and industry-specific compliance standards and participates in rigorous third-party audits, which verify our security controls.

Our customers maintain full ownership and control over their own data.

Microsoft Azure's security SLA can be seen at: https://azure.microsoft.com/en-gb/support/legal/sla/

Physical Access

Optima's customer data is hosted in Microsoft Azure data centres. Microsoft designs, builds, and operates data centres in a way that strictly controls physical access to the areas where data is stored. Tall fences made of steel and concrete encompass every inch of the perimeter and there are cameras around the data centres, with a security team monitoring their videos at all times. Full information related to these controls can be seen here: Microsoft Datacentre Physical Access Security.

Optima employees work remotely and security is applied through technical controls, access control, network security, policies and training. Optima employees can only access the customer environment via VPN connection.

Hosting Availability

Customer data is hosted by Microsoft Azure and therefore Optima utilises their 99.9% uptime resilience within its customer operations. Virtual servers in the Optima's live environment and corporate network utilise storage containers. Each storage container implements redundancy. This can be locally redundant or geo-redundant.

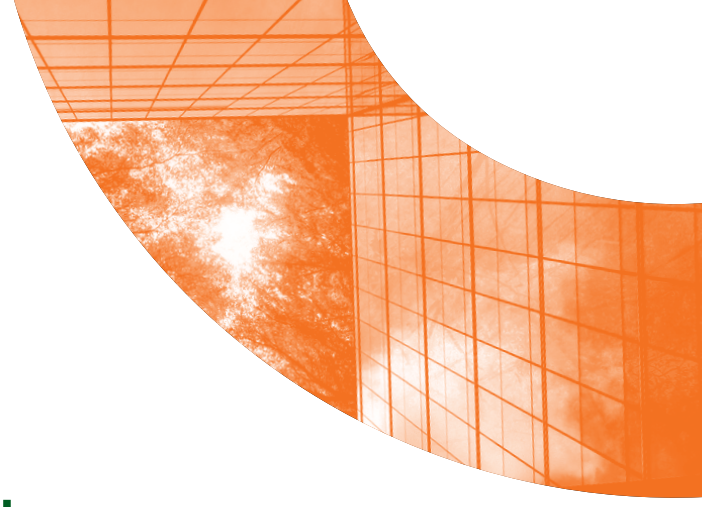
Business Continuity

Optima has implemented a business continuity management system which is accredited with BS EN ISO 22301:2019, the objectives for which are to ensure uptime and availability of our products to our customers, to ensure we are able to continue delivering customer service and to continually improve our approach to business continuity.

Optima has completed a business impact analysis, which is regularly reviewed, in order to prioritise the top-level processes and business functions that would need to be restored in the event of a disaster. A risk assessment of potential incidents which would affect the business has been carried out, resulting in the implementation of business continuity strategies to reduce the impact and the recovery time in the event of a disaster.

Business continuity plans are exercised each year. This includes either live testing of the plans, or scenario-based simulations and walkthroughs to check for consistency and accuracy of the documented plans and procedures.

A copy of our ISO 22301 certificate can be obtained on request.



Technological Security

Network Segregation

Optima's environments are located on our cloud-based hosting with Microsoft Azure on separate subnets to reduce the risk of unauthorised access or changes to the live system. These environments are within separate network address spaces hosted on separate servers with appropriate access control.

Optima's environments are:

1. Live Operational Environment (Prod) - Customer facing
2. Development & Test Environment (Staging) - Internal

User Access Control

Optima controls access to its products via a licensing model. Our customers are able to define the level of privileges for their users - as required by their system administrator - which is then configured by Optima as the Main User.

Backups

Customer databases are backed up using specialist backup software in order to allow for point-in-time data restores. Full database backups are run weekly and transaction log backups every few hours. These are retained for a period of time should they need to be restored. Backups are tested automatically each week.

Multi-Factor Authentication

Multi-factor authentication functionality is available in our cloud application and can be defined at the customer level. Our customers have the option to make MFA mandatory for all users or optional depending on their preference.

Encryption

Appropriate encryption and authentication are applied to Optima's software products at the transport level. For internally facing applications, authentication will be applied if the system contains data that needs to be restricted.

SSL certificates for domains managed by Optima are monitored and reviewed and will expire at the end of their lifecycle, to be replaced when renewal is due. SSL certificates may also be renewed to reflect changes in security standards and requirements.

Secure Development

Optima is committed to producing stable, secure products that protect both Optima and our customers. Security is a key part of our software development and lifecycle (SDLC) which incorporates the whole development process from concept through to deployment of our products. Optima has a Secure Development Policy and Development Handbook, detailing the following areas:

- Guidance on security in our software development lifecycle, the standards and best practice for coding in various languages and technologies;
- How we manage security in our development environment, how our source code is managed and secured and the different dev, test, and production environments;
- The coding guidelines for each of the programming languages we use, the required application security knowledge and tools to help developers find and fix vulnerabilities

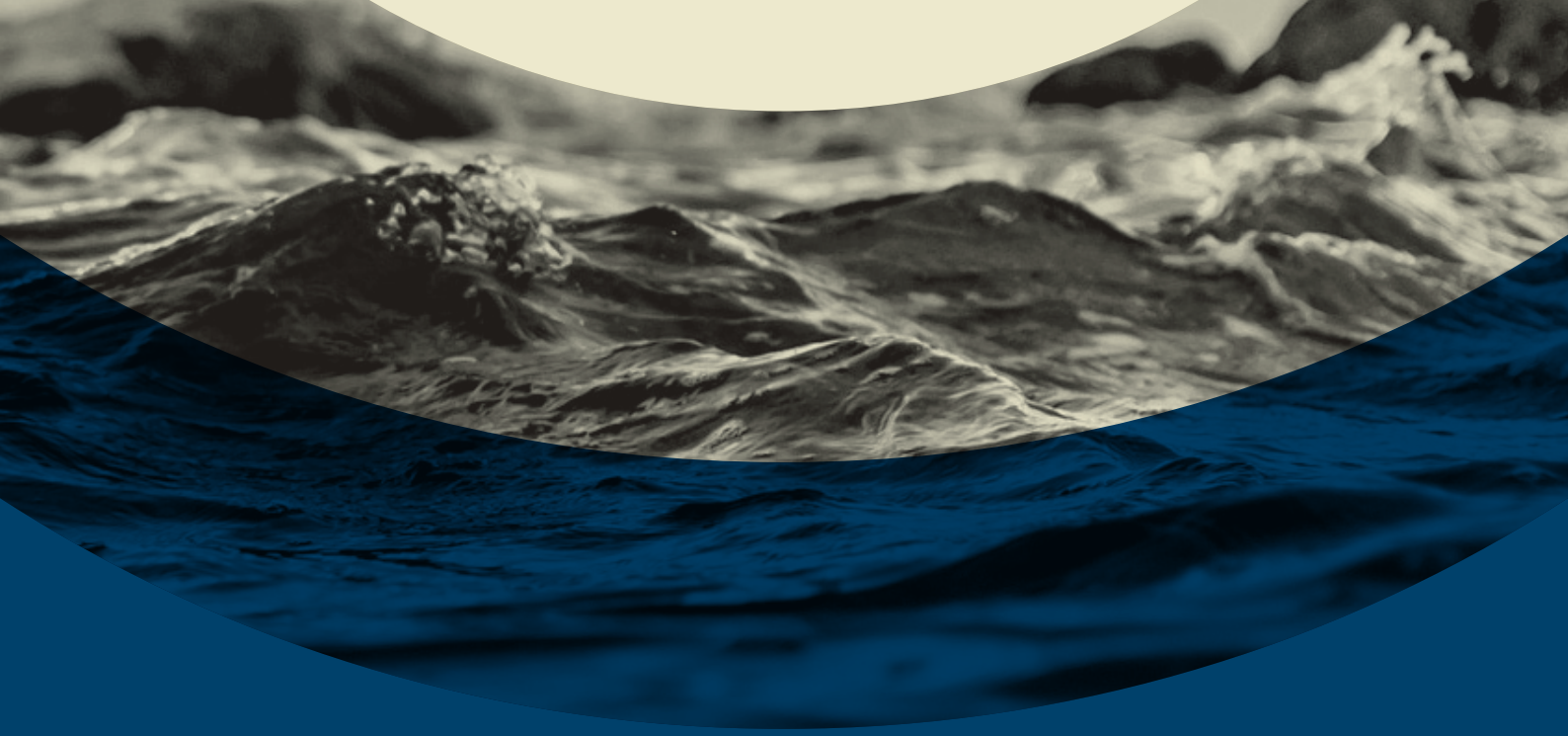
Penetration Testing

Our web applications are independently tested by CHECK accredited pen testers on an annual basis. The results of these tests are shared with senior management and the development team to remediate within a timely manner. Our Compliance Manager can provide executive summaries of these tests to our customers on request.

Incident Management

Incidents are initiated when there is an impact on the confidentiality, integrity or availability of data. We have defined a process for resolving security incidents which encompass the procedure from raising the issue through to investigation and corrective actions. This process is communicated to all employees and refreshers are given at quarterly staff briefings. In the event of an incident that affects customers, the organisation will be informed promptly by our customer service team.

After each incident has been resolved, a root cause analysis meeting is held to identify the causes of the incident, to assess its impact, identify any trends and to ensure the correction and corrective actions are defined. The information security management system may be altered with additional controls, audits or policy revisions may arise from the root cause analysis meetings. If we feel that communication with our customers is required, this is undertaken by our Customer Success Managers.



optima
technology

Information Security Management ISO 27001 Certified

bsi. ISO/IEC 27001 Information Security Management
600872

CYBER ESSENTIALS PLUS

info@optimatech.io | www.optimatech.io